WHAT IS CLAIMED IS:

1. A method of securely storing and transmitting data between a data server and a client, said method comprising:

storing a first set of data on said data server, said first set of data being encrypted by a first private key;

establishing a set of rules for responding to a data request from said client, and storing said rules on said data server;

upon receiving said data request from said client, transmitting an authentication request from said data server to said security server;

authenticating said user responsive to said authentication request;

generating a first private key at said security server, said first private key associated with said data server;

generating a second private key at said security server, said second private key associated with said client; and

generating a session key at said security server.

2. The method of claim 1, further comprising:

encrypting said session key with said first private key, thereby generating a first encrypted session key;

encrypting said session key with said second private key, thereby generating a second encrypted session key;

transmitting said first encrypted session key and said second encrypted session key to said data server; and

transmitting said second encrypted session key to said client.

3. The method of claim 2, further comprising transmitting said second encrypted session key to said data server.

4. The method of claim 2, further comprising:

decrypting said session key using said first private key at said data server;

decrypting said second private key using said session key at said data server;

encrypting a second set of data, said second set of data being a subset of said first set of data and responsive to said data request, using said session key and said second private key, thereby generating a set of encrypted data;

transmitting said set of encrypted data to said client.

5. The method of claim 4, further comprising:

decrypting said session key using said second private key at said client;

decrypting said set of encrypted data using said session key at said client.

6. The method of claim 6, further comprising:

decrypting said set of encrypted data using said second private key at said client.

6. A system for securely storing and transmitting data comprising:

a data server, said data server having an encryption/decryption engine and a first private cipher, wherein said data server is configured to respond to a data request from said user device;

a user device in electrical communication with said data server for sending said data request and receiving a set of responsive data, said user device having a second private cipher; and

a security server having a third private cipher, said security server in communication with said user device and said data server, wherein said security server established a secure transmission link.

7. The system for securely transmitting data of claim 6, wherein said data server further comprises a PCI board for hosting the encryption/decryption engine.

8. The system for securely storing and transmitting data of claim 7, wherein said PCI board comprises an erasable memory for storing said second encryption key.

9. The system for securely storing and transmitting data of claim 8, wherein said erasable memory is flash memory.

10. The system for securely storing and transmitting data of claim 6, wherein said second private cipher is stored in said user device in a hardware format.

11. The system for securely storing and transmitting data of claim 6, wherein said third private cipher is randomly generated.

12. The system for securely storing and transmitting data of claim 11, wherein said randomly generated third private cipher is unique to a secure data transmission session.

13. The system for securely storing and transmitting data of claim 6, wherein said data server contains a set of files, and at least some of said files are encrypted using said first private cipher.

14. The system for securely storing and transmitting data of claim 13, wherein substantially all of said files are encrypted using said private cipher.

15. The system for securely storing and transmitting data of claim 6, wherein said first private cipher is not stored in memory.

16. The system for securely storing and transmitting data of claim 15, wherein said first private cipher is not accessible on any bus.

17. A method of creating a secure data transmission session comprising:

generating a random session key at a security server;

validating a data server and a user device requesting said secure data transmission session;

generating a first secret key for said data server;

generating a second secret key for said user device;

encrypting said random session key with said first secret key, resulting in a first encrypted random session key, and transmitting said first encrypted random session key to said data server;

encrypting said random session key with said second secret key, resulting in a second encrypted random session key, and transmitting said second encrypted random session key to said user device; and

transmitting data from said data sever to said user device via said secure data transmission session.

18. The method of claim 17, wherein said random session key is hardware generated.

19. The method of claim 18, wherein said hardware used for generating said random session key is reconfigurable.

20. The method of claim 17, wherein said first secret key is hardware generated.

21. The method of claim 20, wherein said hardware used for generating said first secret key is reconfigurable.

22. The method of claim 17, wherein said second secret key is hardware generated.

23. The method of claim 22, wherein said hardware used for generating said second secret key is reconfigurable.

24. The method of claim 17, further comprising decrypting said data using said random session key, said first secret key and said second secret key.